Wage Record Interchange System (WRIS)

Standard Operating Procedures

Washington State Employment Security Department

September 2009

Background

The Wage Record Interchange System (WRIS) is a clearinghouse for state Unemployment Insurance (UI) wage data. It is an automated system that has been developed to facilitate the interstate exchange of UI wage data between participating states for the purpose of assessing and reporting on state and local performance for programs authorized under the Workforce Investment Act of 1998 (WIA), under other statutory provisions authorizing programs identified as One-Stop partners in the WIA, and for other purposes allowed under law. Specifically, the WRIS: 1) assists states in assessing the performance of individual training providers and state employment and training programs; 2) supports states in preparing and submitting reports to the U.S. Department of Labor (USDOL) regarding the performance of workforce investment programs and activities authorized under the WIA, or under other statutory provisions that are referenced in the WIA as authorizing programs identified as One-Stop partners; and 3) supports research and evaluation efforts.

The Employment & Training Administration within the U.S. Department of Labor conducts a compliance visit once every three years to verify that WRIS data is being protected according to federal confidentiality standards. An annual internal review will be conducted to confirm that WRIS data is being appropriately protected according to established procedures.

Purpose

The protection of confidential information is of the highest priority for Employment Security Department (ESD). The purpose of the Standard Operating Procedures is to document established procedures for Washington State to show compliance with DOL requirements for the protection of confidential information disclosed through the WRIS by all participating parties. WRIS data can only be used for authorized purposes, disclosed only to authorized persons, and reported appropriately, and must be flagged if commingled with other data in a common database; i.e. data aggregation rules are being followed and destroyed in a timely manner using appropriate methods.

Other WRIS Compliance Documents

The WRIS Data Sharing Agreement (as amended April 9, 2008) details the operating conditions and procedures that govern the participation of State Unemployment Insurance Agencies (SUIA) that hold wage data, state Performance Accountability and Customer Information Agencies (PACIAs) that use wage data, and USDOL-ETA in the WRIS and to establish certain conditions and procedures, consistent with 20 CFR Part 603, that are intended to protect the confidentiality of information disclosed among the participating parties through the WRIS. The Data Sharing Agreement (DSA) defines the roles and responsibilities of the parties, confidentiality and restrictions on the use of information and the operation of the WRIS. It includes a list of terms

with definitions that pertain specifically to WRIS, http://www.doleta.gov/performance/WRISData_Sharing_Agreement_As_Amended_April_9_2008.doc.

The WRIS Confidentiality Compliance Review and Incident Response Training Module describes the purpose and operation of the WRIS Confidentiality Compliance Reviews, the value of and procedures for self-assessment for data confidentiality and system security, and requirements for incident response including developing an incident response plan. This Webinar will be sent to each WRIS user.

New agency employees are required to attend an ethics training course that includes protection of confidential information in all facets of work performed by ESD. This training must be retaken every five years. Agency polices cover specific handling, storage and destruction of confidential information. (See attached Administrative Policy No. 0031): http://inside.esd.wa.gov/policies/0000/PP_0031.pdf and Title 50 RCW Unemployment Compensation RCW Depositions 50.13: http://apps.leg.wa.gov/RCW/default.aspx?cite=50.13&full=true.

Protection of Confidentiality

WRIS use must be limited to authorized individuals who must handle data in a manner that will prevent loss, misuse and unauthorized access to or modification of the information. All WRIS authorized users are required to follow the WRIS Standard Operating Procedures and the terms of the WRIS Data Sharing Agreement.

The WRIS Data Sharing Agreement is signed and dated by Washington's SUIA and PACIA, acknowledging that the state understands and accepts the terms of the Agreement.

WRIS users must read the WRIS Data Sharing Agreement and subsequently sign and date a WRIS Access Acknowledgement form attesting that they have read, understood and accepted the terms of the agreement. A copy of the signed form is stored electronically by a PACIA. When there is an amendment to the DSA it will be presented to WRIS users for review, signature and date to acknowledge reading, understanding and accepting the terms of the amendment, http://www.doleta.gov/performance/PACIA-SUIA-Access_Acknowledgement_n1.pdf.

To access the WRIS system you must have an authorized WRIS User Name and Password from DOLETA. After a WRIS Password has been assigned to an authorized employee, the Password can be written down, but it cannot be written on a copy of the WRIS Access Acknowledgment form. The written record of the Password must be kept secure and confidential.

The DOLETA contact for WRIS, wris@dol.gov, must be notified at once to cancel the account if there is a concern that the confidentiality of user names, passwords or other information may have been compromised. A new Username, Password and access to the system will be activated.

New Information and Training

Pertinent information in the form of instructions from DOLETA, and recommendations for improvement by the WRIS Advisory Group will be made available to PACIA, SUIA and WRIS users for training. Staff will be notified when training tools, for example Webinars, are made available and encouraged to attend or to review on DOL's website.

Change in Status for WRIS Users

DOLETA (WRIS administrator) and ACS (WRIS operator) will be notified by phone and email when authorized employees retire, resign or are reassigned in order to have their WRIS access terminated. It is the responsibility of WRIS users to notify the PACIA representative or the WRIS coordinator when they will no longer need access to WRIS.

Use of WRIS Data

The Wage Data obtained through the WRIS Clearinghouse will be processed and handled to protect the confidentiality of the data, and to prevent unauthorized persons from retrieving such records by computer, remote terminal, or any other means.

No employee of the SUIA receiving a Query may duplicate or disseminate the Wage Data contained in the Query except to other employees specifically authorized to receive such data. Wage data may not be duplicated or disseminated to anyone outside the SUIA. The Query will be retained only for the period of time required to respond with a Reply, electronic data shall be permanently deleted. A separate file or system can not be created for the SSNs of individuals from a Query for Wage Data. Replies transmitted from the SUIA to the WRIS Clearinghouse shall be stored in an area that is physically safe from access by unauthorized persons at all times. The Queries obtained through the WRIS shall be processed in a manner that will protect the confidentiality of the records, and in such a way that unauthorized persons cannot retrieve such records by means of computer, remote terminal, or any other means.

The PACIA will not share Wage Data obtained through the WRIS with any party outside the PACIA except in the form of Aggregate Statistical Reports and under authorized conditions defined in the WRIS DSA under Section VIII, Confidentiality/Restrictions on Use of Information under B. 1, PACIA. A separate file or system will not be created for Wage Data provided by the SUIA. Wage Data shall be retained for only the period of time required to utilize it for assessment and reporting purposes, or for federal records per retention requirement. Thereafter, the Wage Data shall be destroyed and electronic data permanently deleted. Information used to create Requests must be obtained and transmitted according to FERPA policy and state laws governing the confidentiality of information in the possession of educational institutions.

WRIS data (i.e. passwords, wages, SSNs, etc.) are not to be included in any communication that can be seen, or intercepted, by anyone who is not authorized to view them, except in aggregate form.

Commingled WRIS data
Wage data included in any interconnected databases must be flagged. This data must be used and protected as defined in the WRIS Standard Operating Procedures and the WRIS Data Sharing Agreement.

Remoting into Computers
WRIS users that remote into their computer and view WRIS data may not store this data on a laptop, flash drive or on any device that could be lost or taken.

Physical Security
Public access to offices where WRIS data are held and used should be restricted. Workspaces are to be configured to prevent unauthorized staff from viewing computer screens. Computers assigned to WRIS authorized users cannot be used by any other staff. WRIS authorized users must lock their computers when they step away from their work area.

Storage of Confidential Data
Wage data obtained through WRIS must be stored securely and protected from access by unauthorized persons at all times.

Retention of Confidential Data
Printed WRIS data may only be stored as long as needed. Data stored on hard drives, diskettes, CDs, tapes, or other electronic media should be stored only as long as needed.

Proper Disposal and Destruction of Confidential Data
WRIS data must be shredded by the WRIS authorized user; it cannot be discarded intact in either unlocked or locked recycling bins for disposal and/or destruction by another party. Confidential and sensitive data is to be deleted from hard drives, diskettes, CDs, tapes, or other electronic media when no longer needed.

Destruction Log
WRIS data must be destroyed when the data is no longer needed. Destruction of WRIS data either by shredding of paper or destruction of magnetic discs or files must be documented in the destruction log. A copy of the Destruction Log is attached to the SOPs in Word format. The Destruction Log can be maintained electronically or printed. The Destruction Log must be available for viewing if requested.

Incident Response Plan

Incident response allows an agency to mobilize all necessary resources as quickly as possible and minimizes agency damage. Incident response promotes a quick return to normal operations.

The DOLETA contact for WRIS, wris@dol.gov, must be notified at once to immediately terminate access to WRIS if it is appropriate because there is a concern that the confidentiality of user names, passwords or other information may have been compromised. A new Username, Password and access to the system will be activated.

In the event of a breach of confidentiality due to inadvertent misuse or disclosure of WRIS data, WRIS authorized users must notify their supervisor and the state WRIS coordinator of the incident as soon as possible. The state WRIS coordinator and/or the PACIA will subsequently inform WRIS Administrator DOLETA and WRIS Operator ACS of the state's corrective action response and resolution.

Continuing Education

The continuous education of WRIS users is the most effective tool in place to prevent a breach of confidentiality. That education shall include (1) reading, asking questions about, and understanding the WRIS Data Sharing Agreement (as documented by a signed and dated WRIS Access Acknowledgement form); (2) reading, asking questions about, and understanding the WRIS Standard Operating Procedures; and (3) attending DOLETA sponsored WRIS webinars related to WRIS data use, security and confidentiality.

Confidentiality Compliance Review self-assessment focuses on maintaining the security and integrity of WRIS wage data, appropriate use, authorized disclosure and physical security. A compliance review by the DOLETA WRIS Administration once every three years ensures data is protected according to standards of the DSA. Technical and administrative assistance is available at that time.

An internal Confidentiality Compliance Review will be conducted annually to provide an opportunity to identify issues. A report will be written and distributed to the PACIA.

Direct Inquiries to:

Susan Haerling
WorkSource Standards and Integration Division
Employment Security Department
PO Box 9046, MS 6000
Olympia, WA 98507-9046
E-Mail: shaerling@esd.wa.gov
Telephone: (360) 438-4040
Fax: (360) 438-3174

DOL WRIS website: http://www.doleta.gov/performance/WRIS.cfm